(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－289255

(43)公開日　平成11年(1999)10月19日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０３Ｍ　7/00		Ｈ０３Ｍ	7/00	
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ	5/00	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ	20/10	Ｈ
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ	1/387	

審査請求　未請求　請求項の数35　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－14937

(22)出願日　平成11年(1999)１月22日

(31)優先権主張番号　特願平10－18667

(32)優先日　平10(1998)１月30日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

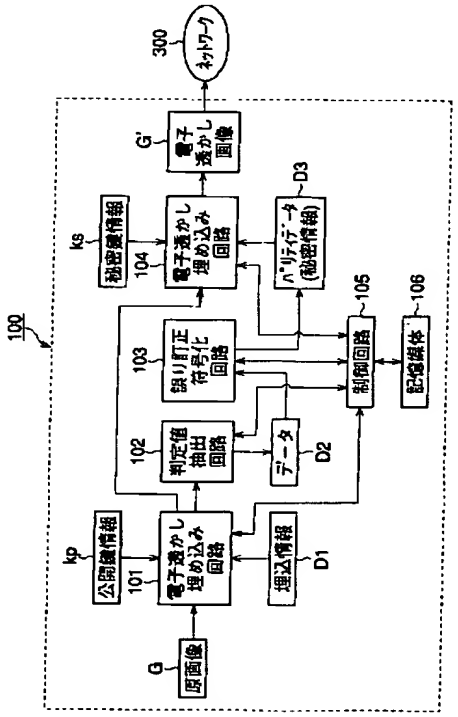
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　電子機器、データ処理方法、電子透かし方式、データ処理システム、及び記憶媒体

(57)【要約】

【課題】　一般のユーザによる自由な電子透かし情報の抽出と、ディジタルデータの著作権の保護とを同時に満たすことが可能な著作権保護技術を用いたデータ処理システムを提供する。

【解決手段】　第１の埋込手段１０１は、公開鍵ｋｐを用いて第１の情報Ｄ１をディジタルデータＧに対して埋め込む。第２の埋込手段１０４は、第１の情報Ｄ１を復元するための第２の情報Ｄ３を埋め込む。この結果（ディジタルデータＧ’）の受取側は、公開鍵ｋｐを用いてディジタルデータＧ’から第１の情報Ｄ１を自由に抽出することができ、ディジタルデータＧ’の第１の情報Ｄ１が破壊されていたとしても、これを第２の情報Ｄ３によって復元することができる。



1

【特許請求の範囲】

【請求項１】　ディジタルデータに対して第１の情報を埋め込む第１の埋込手段と、上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込手段とを備えることを特徴とする電子機器。

【請求項２】　上記第１の情報及び上記第２の情報の埋込対象となる上記ディジタルデータは、複数の領域に分割されており、それぞれの領域間に所定の関係を有することを特徴とする請求項１記載の電子機器。

【請求項３】　上記複数の領域は、上記第１の情報が埋め込まれる第１の領域と、上記第２の情報が埋め込まれる第２の領域と、上記第１及び第２の情報が埋め込まれない第３の領域とをを含むことを特徴とする請求項２記載の電子機器。

【請求項４】　上記第２の情報は、上記第１の領域及び上記第３の領域から検出される各データに基づいて生成されることを特徴とする請求項３記載の電子機器。

【請求項５】　上記複数の領域は、複数の実空間領域と複数の周波数領域の何れかの領域を含むことを特徴とする請求項２記載の電子機器。

【請求項６】　上記第２の情報は、誤り訂正符号化処理によって生成されることを特徴とする請求項１記載の電子楽器。

【請求項７】　上記第１の情報は、上記ディジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする請求項１記載の電子機器。

【請求項８】　上記第１の埋込手段は、離散コサイン変換、フーリエ変換、及びウェーブレット変換の少なくとも１つを用いて上記第１の情報を埋め込むことを特徴とする請求項１記載の電子機器。

【請求項９】　上記第１の埋込手段は、上記ディジタルデータが有する変数を操作することによって上記第１の情報を埋め込むことを特徴とする請求項１記載の電子機器。

【請求項１０】　上記変数は、ディジタル画像データの輝度成分を含むことを特徴とする請求項９記載の電子機器。

【請求項１１】　上記第１の埋込手段での上記第１の情報を埋め込む方法と、上記第２の埋込手段での上記第２の情報を埋め込む方法とが異なることを特徴とする請求項１記載の電子機器。

【請求項１２】　上記第１の情報を埋め込むために必要な鍵情報が公開されていることを特徴とする請求項１記載の電子機器。

【請求項１３】　上記第２の情報を埋め込むために必要な鍵情報が公開されていないことを特徴とする請求項１記載の電子機器。

【請求項１４】　パーソナルコンピュータ、ディジタル

2

カメラ、ディジタルビデオレコーダ、カメラ一体型ディジタルレコーダ、スキャナ、及び画像ファイル装置の少なくとも１つに備えたことを特徴とする請求項１記載の電子機器。

【請求項１５】　上記ディジタルデータは、画像データを含むことを特徴とする請求項１記載の電子機器。

【請求項１６】　上記ディジタルデータは、音声データ、グラフィックスデータ、テキストデータ、及びプログラムデータの少なくとも１つを含むことを特徴とする請求項１記載の電子機器。

【請求項１７】　ディジタルデータに対して第１の情報を埋め込む第１の埋込ステップと、

上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込ステップとを含むことを特徴とするデータ処理方法。

【請求項１８】　第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出手段と、

上記抽出手段にて得られた上記第２の情報に基づいて、上記第１の情報を復元する復元手段とを備えることを特徴とする電子機器。

【請求項１９】　第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出ステップと、上記抽出ステップにより得られた上記第２の情報に基づいて、上記第１の情報を復元する復元ステップとを含むことを特徴とするデータ処理方法。

【請求項２０】　ディジタルデータを入力する入力手段と、

公開された鍵情報を用いて上記ディジタルデータに所定の情報を埋め込む埋込手段とを備えることを特徴とする電子機器。

【請求項２１】　上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込む手段を更に備えることを特徴とする請求項２０記載の電子機器。

【請求項２２】　ディジタルデータを入力する入力ステップと、

公開された鍵情報を用いて上記ディジタルデータに所定の情報を埋め込む埋込ステップとを含むことを特徴とするデータ処理方法。

【請求項２３】　上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込むステップを更に含むことを特徴とする請求項２２記載のデータ処理方法。

【請求項２４】　ディジタルデータを入力する入力手段と、

公開された鍵情報を用いて上記ディジタルデータから所定の情報を抽出する抽出手段とを備えることを特徴とする電子機器。

【請求項２５】　上記ディジタルデータから検出される

秘密情報に基づいて、上記所定の情報を復元する復元手段を備えることを特徴とする請求項２４記載の電子機器。

【請求項２６】　ディジタルデータを入力する入力ステップと、

公開された鍵情報を用いて上記ディジタルデータから所定の情報を抽出する抽出ステップとを含むことを特徴とするデータ処理方法。

【請求項２７】　上記ディジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元ステップを含むことを特徴とする請求項２６記載のデータ処理方法。

【請求項２８】　公開された鍵情報を用いて、ディジタルデータに所定の情報を埋め込む第１の装置と、

上記公開された鍵情報を用いて、上記ディジタルデータに埋め込まれた所定の情報を抽出する第２の装置とを含むことを特徴とするデータ処理システム。

【請求項２９】　上記第１の装置は、上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込み、

上記第２の装置は、上記秘密情報に基づいて、上記所定の情報を復元することを特徴とする請求項２８記載のデータ処理システム。

【請求項３０】　上記所定の情報は、上記ディジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする請求項２８記載のデータ処理システム。

【請求項３１】　著作権保護システムに備えたことを特徴とする請求項２８記載のデータ処理システム。

【請求項３２】　電子商取引システム及びディジタルデータ配布システムの少なくとも何れかのシステムに備えたことを特徴とする請求項２８記載のデータ処理システム。

【請求項３３】　ディジタルデータに対して第１の情報を埋め込む第１の埋込工程と、

上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする記憶媒体。

【請求項３４】　第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出工程と、

上記抽出工程により抽出された上記第２の情報に基づいて、上記第１の情報を復元する復元工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする記憶媒体。

【請求項３５】　公開鍵を用いた電子透かし埋込処理により、原データに情報を埋め込む埋込工程と、

上記公開鍵を用いて、上記原データに埋め込まれた情報を抽出する抽出工程との少なくとも何れかの工程を含むことを特徴とする電子透かし方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子機器、データ処理方法、データ処理システム、及びコンピュータ読出可能な記憶媒体に関し、例えば、各種のディジタル情報の著作権を保護するための技術、或いは著作権を保護するための技術を用いたディジタル情報配布システムや電子商取引システムに適用される電子機器、データ処理方法、データ処理システム、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体に関するものである。

【０００２】

【従来の技術】近年のコンピュータネットワークの発達や、安価で高性能なコンピュータの普及により、近い将来、ネットワーク上で商品の売買を行うサービスである所謂「電子商取引」が盛んになると考えられている。この電子商取引で売買される商品は、例えば、静止画像等のディジタルデータである。しかしながら、電子商取引を実現するためには、解決しなければならない問題がいくつかある。その一つとして、例えば、ディジタルデータは一般的に、完全なコピーを容易且つ大量に作成でき、その内容の変更も簡単にできるという性質を持っている。このため、ディジタルデータからなる商品を買ったユーザが、オリジナルと同質のコピーデータ（複製）を不正に作成し、それを他のユーザに再配布してしまう可能性がある。この場合、その商品の著作権者又はその著作権者から正当に販売を委託された者（以下、「販売者」と言う）は、その商品に支払われるべき代価を受け取ることができないという問題が生じてくる。

【０００３】一方、著作権者又は販売者（以下、ディジタルデータからなる商品を正当に配布する側をまとめて「サーバ」と言う）が、一度購入者に対して商品を送ってしまうと、その商品の不正なコピーや内容の改ざん等を完全に防止することができないため、その商品の著作権が侵害されるという問題が生じてくる。そこで、このような電子商取引上の問題を解決する技術として、現在、「電子透かし」と呼ばれる技術が研究されている。「電子透かし」とは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する著作権情報や購入者に関するユーザ情報を、ディジタルデータ自体に目に見えないように埋め込む技術である。この技術を応用することによって、例えば、不正コピーが発見された場合に、誰がその不正コピーを再配布したのかを特定することができる。　また、「電子透かし」の技術を実現する手法としては、現在、離散コサイン変換、フーリエ変換、ウェーブレット変換等を用いて、ある特定の周波数領域を操作する手法や、画素の輝度値を直接操作する手法が研究されている。

【０００４】上述のような電子透かし技術の安全性と信

頼性は、ディジタルデータに埋め込まれた情報が不可視であるということと、その情報の埋め込み場所と埋め込み強度とに関する鍵情報がわからなければ、その情報を破壊したり、内容を変更したりすることができないということとから成り立っている。例えば、「B. Pfitmann and M. Waidner : Asymmetic Fingerprinting, EUROCRYPT 96」には、画像毎に、その画像を購入したユーザの情報を埋込情報として埋め込むことで、不正配布を特定できるシステムが提案されている。しかしながら、このようなシステムにおいても、上記の埋込情報の鍵情報が公開されれば、不正なユーザはその埋込情報を破壊したり、変形したりすることができてしまう。このような問題を解決するために、次のような構成が考えられている。

【０００５】まず、図１４は、電子透かし技術を用いたシステム９００の一例を示したものである。この図１４において、埋込側９１０の電子透かし埋め込み回路９１１は、鍵情報ｋを用いてオリジナルの画像データＧに埋込情報Ｄを埋め込む。ここで、鍵情報ｋは、埋込情報Ｄを抽出するために必要な情報であって、例えば、埋込情報Ｄの埋め込み場所や埋め込み強度等の情報である。埋込情報Ｄの埋め込まれた画像データＧは、電子透かし画像データとして外部に送出される。一方、抽出側９２０の電子透かし抽出回路９２１は、埋込側９１０の鍵情報ｋと同じ鍵情報ｋを用いて、上記の電子透かし画像データから埋込情報Ｄを抽出する。このように、上記図１４のシステム９００では、埋込側９１０と抽出側９２０とで共通の鍵情報ｋを用いて、電子透かしである埋込情報Ｄの埋込及び抽出を行うように構成されている。

【０００６】そこで、上記図１４のシステム９００において、上述した不正な処理を防止するためには、埋込情報Ｄの埋め込み場所や埋め込み強度等に関する鍵情報ｋを、埋込側９１０と抽出側９２０の何れにおいても秘密に保つ必要がある。このため、上記図１４のシステム９００では、埋込情報Ｄの抽出を、鍵情報ｋを生成した鍵情報管理機関や、鍵情報ｋを知ることのできる特別な検査機関においてのみ行うように構成することが考えられている。したがって、これらの機関が、不正に再配布されたディジタルデータや内容の変更されたディジタルデータを監視することによって、著作権者の権利の保護を実現することができる。

【０００７】尚、上記図１４に示したようなシステム９００の構成は、暗号化技術のアナロジーで考えると、暗号化を行うための暗号鍵とその暗号化を復号するための復号鍵とが同じ鍵となる共通鍵暗号化方式的な手法による構成であると言える。

【０００８】

【発明が解決しようとする課題】しかしながら、上記図１４のシステム９００では、埋込情報Ｄを抽出するために必要な鍵情報ｋを、埋め込み側９１０と抽出側９２０とで共に秘密に管理する必要があったため、ネットワークを介して自由に送受信することはできなかった。また、埋込情報Ｄの抽出は、上述したような特殊な機関のみでしか行うことができないように構成されていた。したがって、一般の各ユーザは、埋込情報Ｄを自由に抽出することができなかったため、外部から入手したディジタルデータの著作権の内容やその正当性を確認することができず、大変不便であるという問題があった。

【０００９】上記の問題を解決するためには、例えば、埋込情報Ｄを抽出するために必要な鍵情報ｋを、抽出側９２０の電子機器を製造するメーカを含めた一般のユーザに対して公開する必要がある。しかしながら、このような構成、すなわち鍵情報ｋを公開する構成とすれば、上述したような不正な処理によってディジタルデータの著作権が損なわれる恐れがある。つまり、単に鍵情報ｋを公開するだけでは、一般のユーザの誰もが自由に埋込情報Ｄを確認することはできるが、埋込情報Ｄによってディジタルデータの著作権を十分に保護することはできない。

【００１０】上述のように、従来の電子透かし技術では、電子透かしである埋込情報Ｄの抽出に必要な鍵情報ｋを秘密に管理することなく、一般のユーザによる自由な電子透かしの抽出とディジタルデータの著作権の保護とを同時に満たすことのできる手法は提案されていなかった。また、このような電子透かし技術を適用した著作権保護のための技術も、その著作権保護技術を用いて構成された電子商取引システムやディジタル情報配布システムも提案されていなかった。

【００１１】そこで、本発明は、上記の欠点を除去するために成されたもので、一般のユーザによる自由な電子透かし情報の抽出と、ディジタルデータの著作権の保護とを同時に満たすことが可能な著作権保護技術を用いた電子機器、データ処理方法、データ処理システム、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体を提供することを目的とする。

【００１２】

【課題を解決するための手段】斯かる目的下において、第１の発明は、ディジタルデータに対して第１の情報を埋め込む第１の埋込手段と、上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込手段とを備えることを特徴とする。

【００１３】第２の発明は、上記第１の発明において、上記第１の情報及び上記第２の情報の埋込対象となる上記ディジタルデータは、複数の領域に分割されており、それぞれの領域間に所定の関係を有することを特徴とする。

【００１４】第３の発明は、上記第２の発明において、上記複数の領域は、上記第１の情報が埋め込まれる第１の領域と、上記第２の情報が埋め込まれる第２の領域

と、上記第１及び第２の情報が埋め込まれない第３の領域とをを含むことを特徴とする。

【００１５】第４の発明は、上記第３の発明において、上記第２の情報は、上記第１の領域及び上記第３の領域から検出される各データに基づいて生成されることを特徴とする。

【００１６】第５の発明は、上記第２の発明において、上記複数の領域は、複数の実空間領域と複数の周波数領域の何れかの領域を含むことを特徴とする。

【００１７】第６の発明は、上記第１の発明において、上記第２の情報は、誤り訂正符号化処理によって生成されることを特徴とする。

【００１８】第７の発明は、上記第１の発明において、上記第１の情報は、上記ディジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする。

【００１９】第８の発明は、上記第１の発明において、上記第１の埋込手段は、離散コサイン変換、フーリエ変換、及びウェーブレット変換の少なくとも１つを用いて上記第１の情報を埋め込むことを特徴とする。

【００２０】第９の発明は、上記第１の発明において、上記第１の埋込手段は、上記ディジタルデータが有する変数を操作することによって上記第１の情報を埋め込むことを特徴とする。

【００２１】第１０の発明は、上記第９の発明において、上記変数は、ディジタル画像データの輝度成分を含むことを特徴とする。

【００２２】第１１の発明は、上記第１の発明において、上記第１の埋込手段での上記第１の情報を埋め込む方法と、上記第２の埋込手段での上記第２の情報を埋め込む方法とが異なることを特徴とする。

【００２３】第１２の発明は、上記第１の発明において、上記第１の情報を埋め込むために必要な鍵情報が公開されていることを特徴とする。

【００２４】第１３の発明は、上記第１の発明において、上記第２の情報を埋め込むために必要な鍵情報が公開されていないことを特徴とする。

【００２５】第１４の発明は、上記第１の発明において、パーソナルコンピュータ、ディジタルカメラ、ディジタルビデオレコーダ、カメラー体型ディジタルレコーダ、スキャナ、及び画像ファイル装置の少なくとも１つに適用されたものであることを特徴とする。

【００２６】第１５の発明は、上記第１の発明において、上記ディジタルデータは、画像データを含むことを特徴とする。

【００２７】第１６の発明は、上記第１の発明において、上記ディジタルデータは、音声データ、グラフィックスデータ、テキストデータ、及びプログラムデータの少なくとも１つを含むことを特徴とする。

【００２８】第１７の発明は、ディジタルデータに対して第１の情報を埋め込む第１の埋込ステップと、上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込ステップとを含むことを特徴とする。

【００２９】第１８の発明は、第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出手段と、上記抽出手段にて得られた上記第２の情報に基づいて、上記第１の情報を復元する復元手段とを備えることを特徴とする。

【００３０】第１９の発明は、第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出ステップと、上記抽出ステップにより得られた上記第２の情報に基づいて、上記第１の情報を復元する復元ステップとを含むことを特徴とする。

【００３１】第２０の発明は、ディジタルデータを入力する入力手段と、公開された鍵情報を用いて上記ディジタルデータに所定の情報を埋め込む埋込手段とを備えることを特徴とする。

【００３２】第２１の発明は、上記第２０の発明において、上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込む手段を更に備えることを特徴とする。

【００３３】第２２の発明は、ディジタルデータを入力する入力ステップと、公開された鍵情報を用いて上記ディジタルデータに所定の情報を埋め込む埋込ステップとを含むことを特徴とする。

【００３４】第２３の発明は、上記第２２の発明において、上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込むステップを更に含むことを特徴とする。

【００３５】第２４の発明は、ディジタルデータを入力する入力手段と、公開された鍵情報を用いて上記ディジタルデータから所定の情報を抽出する抽出手段とを備えることを特徴とする。

【００３６】第２５の発明は、上記第２４の発明において、上記ディジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元手段を備えることを特徴とする。

【００３７】第２６の発明は、ディジタルデータを入力する入力ステップと、公開された鍵情報を用いて上記ディジタルデータから所定の情報を抽出する抽出ステップとを含むことを特徴とする。

【００３８】第２７の発明は、上記第２６の発明において、上記ディジタルデータから検出される秘密情報に基づいて、上記所定の情報を復元する復元ステップを含むことを特徴とする。

【００３９】第２８の発明は、公開された鍵情報を用いて、ディジタルデータに所定の情報を埋め込む第１の装

置と、上記公開された鍵情報を用いて、上記ディジタルデータに埋め込まれた所定の情報を抽出する第２の装置とを含むことを特徴とする。

【００４０】第２９の発明は、上記第２８の発明において、上記第１の装置は、上記所定の情報を復元するための秘密情報を上記ディジタルデータに埋め込み、上記第２の装置は、上記秘密情報に基づいて、上記所定の情報を復元することを特徴とする。

【００４１】第３０の発明は、上記第２８の発明において、上記所定の情報は、上記ディジタルデータの著作権を管理するための情報及び保護するための情報の少なくとも何れかの情報を含むことを特徴とする。

【００４２】第３１の発明は、上記第２８の発明において、著作権保護システムに備えたことを特徴とする。

【００４３】第３２の発明は、上記第２８の発明において、電子商取引システム及びディジタルデータ配布システムの少なくとも何れかのシステムに備えたことを特徴とする。

【００４４】第３３の発明は、ディジタルデータに対して第１の情報を埋め込む第１の埋込工程と、上記第１の情報を復元するための第２の情報を上記ディジタルデータに対して埋め込む第２の埋込工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする。

【００４５】第３４の発明は、第１の情報と、該第１の情報を復元するための第２の情報とが埋め込まれたディジタルデータから該第２の情報を抽出する抽出工程と、上記抽出工程により抽出された上記第２の情報に基づいて、上記第１の情報を復元する復元工程とを実現するためのプログラムを、コンピュータから読出可能に記憶したことを特徴とする。

【００４６】第３５の発明は、公開鍵を用いた電子透かし埋込処理により、原データに情報を埋め込む埋込工程と、上記公開鍵を用いて、上記原データに埋め込まれた情報を抽出する抽出工程との少なくとも何れかの工程を含む電子透かし方式であることを特徴とする。

【００４７】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【００４８】（第１の実施の形態）本発明は、例えば、図１に示すような電子機器（以下、「埋込装置」と言う）１００と、図２に示すような電子機器（以下、「抽出装置」と言う）２００とを含むシステムに適用される。埋込機器１００は、詳細は後述する電子透かし埋め込み機能を有するものであり、抽出装置２００も、詳細は後述する電子透かし抽出機能を有するものである。これらの装置は、公衆回線、インターネット、イーサネット等からなるネットワーク３００を介して接続されている。以下、本実施の形態における埋込装置２００及び抽出装置３００の各構成、及びそれらの処理動作について具体的に説明する。

【００４９】［埋込装置１００の構成］

【００５０】上記図１の埋込装置１００は、パーソナルコンピュータ、ディジタルカメラ、ディジタルビデオレコーダ、カメラ一体型ディジタルレコーダ、スキャナ等の電子機器、或いはこれらの電子機器に接続可能な拡張ユニットである。上記図１に示すように、埋込装置１００は、ディジタル画像データ（原画像データ）Ｇ、公開鍵情報ｋｐ、及び埋込情報Ｄ１が供給される電子透かし埋込回路１０１と、電子透かし埋込回路１０１の出力が供給される判定値抽出回路１０２と、判定値抽出回路１０２の出力（＝データＤ２）が供給される誤り訂正符号化回路１０３と、誤り訂正符号化回路１０３の出力（＝パリティデータＤ３）、秘密鍵情報ｋｓ、及び電子透かし埋込回路１０１の出力（原画像データＧ＋埋込情報Ｄ１）が供給される電子透かし埋込回路１０４とを含んでなる。また、埋込装置１００は更に、詳細は後述する本実施の形態における埋込処理に従って埋込装置１００全体の動作を制御する制御回路１０５と、上記の埋込処理を実現するためのプログラムコードを記憶した記憶媒体１０６とを含んでなる。

【００５１】ここで、公開鍵情報ｋｐは、埋込情報Ｄ１を埋め込むために必要な情報（例えば、埋め込み場所や埋め込み手順を示す）であり、一般に公開されている鍵情報である。例えば、この公開鍵情報ｋｐは、ネットワーク３００に接続された電子機器の電子掲示板やホームページ等によって公開される。また、原画像データＧは、ここでは静止画像や動画像のデータとしている。但し、原画像データＧとしては、静止画像や動画像のデータに限られることはなく、例えば、音声、テキスデータ、グラフィックスデータ、プログラムデータ等のディジタルデータであってもよい。また、埋込情報Ｄ１は、電子透かし情報であって、原画像データＧの著作権を保護したり管理するためのデータである。

【００５２】［抽出装置２００の構成］

【００５３】上記図２の抽出装置２００は、パーソナルコンピュータ、デジタルテレビ等の電子機器、或いはこれらの電子機器に接続可能な拡張ユニットである。上記図２に示すように、抽出装置２００は、埋込情報Ｄ１の埋め込まれた電子透かし画像データＧを入力する電子透かし抽出回路２０１と、電子透かし抽出回路２０１の出力（＝符号系列Ｄ４）が供給される誤り訂正復号回路２０２と、誤り訂正復号回路２０２の出力（＝訂正系列Ｄ５）が供給される電子透かし抽出回路２０３を含んでなる。また、抽出装置２００は更に、詳細は後述する本実施の形態における抽出処理に従って抽出装置２００全体の動作を制御する制御回路２０５と、上記の埋込処理を実現するためのプログラムコードを記憶した記憶媒体２０６とを含んでなる。

【００５４】［埋込装置１００の処理動作］

【００５５】先ず、電子透かし埋込回路１０１は、公開鍵情報ｋｐを用いて原画像データＧを操作し、埋込情報Ｄ１を埋め込む。

【００５６】ここで、本実施の形態では、埋込情報Ｄ１を抽出するための公開鍵情報ｋｐは、上述したように一般に公開されているため、上述した特殊な機関（鍵情報を生成した鍵情報管理機関や、鍵情報を知ることのできる特別な検査機関等）のみならず、一般のユーザの誰でもが埋込情報Ｄ１の埋め込み位置、埋め込み強度、埋め込み手順等を知ることができると共に、その公開鍵情報ｋｐに基づいて埋込情報Ｄ１を抽出し、その内容を確認することもできる。尚、公開鍵情報ｋｐは、埋込装置１００が外部のネットワーク３００を介して入手する、或いは埋込装置１００内部に予め格納されているものとする。ところが、公開鍵情報ｋｐを公開した場合、不正なユーザが埋込情報Ｄ１を破壊したり、内容を変更したりすることによって、原画像データＧの著作権が損なわれる恐れがある。

【００５７】そこで、本実施の形態での埋込装置１００は、埋込情報Ｄ１の破壊や内容の変更を防止するために、後述する誤り訂正符号化回路１０３及び電子透かし埋め込み回路１０４によって、「秘密情報」を生成して原画像データＧに対して更に埋め込むようになされている。この秘密情報とは、埋込情報Ｄ１を修復するための情報であり、これを用いることによって、抽出装置２００は、破壊、変形、加工された埋込情報Ｄ１を修復することができるようになされている。ここでの埋込情報Ｄ１の修復は、例えば、誤り訂正符号化と復号の手法によって実現することができる。この場合、例えば、上記の秘密情報を、埋込情報Ｄ１を埋め込んだ部分（以下、「公開情報埋込部」と言う）と、埋込情報Ｄ１も秘密情報をも埋め込まない部分（以下、「無情報埋込部」と言う）とから検出されたデータを用いて生成する。また、秘密情報の修復については、公開情報埋込部、秘密情報を埋め込む部分（以下、「秘密情報埋込部」と言う）、及び無情報埋込部の３つの領域から検出されたデータを直接用いて実行される。

【００５８】尚、上述の秘密情報の生成に無情報埋込部から検出されたデータを用いるのは、該秘密情報が原画像データＧのどこに埋め込まれているのかを特定できないようにするためである。

【００５９】次に、判定値抽出回路１０２は、電子透かし埋込回路１０１にて埋込情報Ｄ１が埋め込まれた原画像データＧ（原画像データＧ＋埋込情報Ｄ１）から２つの領域を判別する。すなわち、公開情報埋込部と公開情報埋込部以外の部分を判別する。また、判定値抽出回路１０２は、所定の規則に基づいて、公開情報埋込部以外の部分から秘密情報埋込部と無情報埋込部を決定する。ここで、それぞれの埋込部の領域の大きさは、公開情報埋込部に埋め込まれる埋込情報Ｄ１の情報長、埋込情報Ｄ１を復元するために必要な復元能力（ここでは、誤り訂正能力とする）等に応じて変化する。そして、判定値抽出回路１０２は、所定の規則に基づいて、公開情報埋込部と無情報埋込部からデータＤ２を検出し、このデータＤ２（埋込情報Ｄ１に対応する検出データを含む）を誤り訂正符号化回路１０３に供給する。

【００６０】尚、判定値抽出回路１０２でのデータＤ２を生成する手順については後述する。また、判定値抽出回路１０２を電子透かし埋込回路１０１の後段に設けるように構成したが、詳細は後述するが、判定値抽出回路１０２を電子透かし埋込回路１０１の前段に設けるように構成してもよい。

【００６１】次に、誤り訂正符号化回路１０３は、所定の誤り符号化処理により、判定値抽出回路１０２からのデータＤ２に対する誤り符号（パリティデータ）Ｄ３を生成し、これを上述した埋込情報Ｄ１を修復するための秘密情報Ｄ３として、電子透かし埋め込み回路１０４に供給する。

【００６２】そして、電子透かし埋め込み回路１０４は、誤り訂正符号化回路１０３からの秘密情報Ｄ３（すなわち、パリティデータＤ３）を、判定値抽出回路１０２にて決定された秘密情報埋込部に埋め込み、これを電子透かし画像データＧ’として出力する。

【００６３】上述のようにして、埋込装置１００は、原画像データＧを操作することによって、埋込情報Ｄ１と秘密情報Ｄ３を埋め込んだ電子透かし画像データＧ’（Ｇ＋Ｄ１＋Ｄ３）を生成する。この電子透かし画像データＧ’は、ネットワーク３００を介して抽出装置２００に供給される。

【００６４】［抽出装置２００の処理動作］

【００６５】先ず、電子透かし抽出回路２０１は、埋込装置１００の埋め込み方法に対応する抽出方法に基づいて、詳細は後述するが、埋込装置１００からネットワーク３００を介して供給された電子透かし画像データＧ’から符号系列データＤ４（秘密情報Ｄ３を含む）を抽出し、それを誤り訂正復号回路２０２に供給する。このとき、電子透かし抽出回路２０１は、秘密に管理する必要のない公開鍵情報ｋｐを用いて、電子透かし画像データＧ’から埋込情報Ｄ１のみを抽出することもできる。

【００６６】尚、公開鍵情報ｋｐは、抽出装置２００が外部のネットワーク３００を介して入手する、或いは抽出装置２００の中に予め格納されているものとする。また、電子透かし抽出回路２０１での抽出方法は、埋込装置１００の埋め込み方法に対応するものに限られず、他の方法を用いることも可能である。

【００６７】次に、誤り訂正復号回路２０２は、電子透かし抽出回路２０１からの符号系列データＤ４（＝Ｄ２＋Ｄ３）に含まれるパリティデータＤ３（すなわち、秘密情報Ｄ３）を用いて、それに対応するデータＤ２を誤り訂正復号し、その結果を訂正系列データＤ５として電

子透かし抽出回路２０３に供給する。ここでの処理によって、埋込情報Ｄ１がたとえ破壊されていたとしても、復元することができる。

【００６８】そして、電子透かし抽出回路２０３は、公開鍵情報ｋｐを用いて、誤り訂正復号回路２０２からの訂正系列データＤ５から、埋込情報Ｄ１を検出する。

【００６９】上述のような構成により、抽出装置３００は、秘密情報Ｄ３を用いて電子透かし画像データＧ’から抽出された埋込情報Ｄ１を修復し、復元することができる。また、電子透かし抽出回路２０３にて検出された埋込情報Ｄ１を、次段に設けられている表示部２０４に供給することにより、電子透かし画像データＧ’の著作権情報やユーザ情報等を視覚的に確認することもできる。

【００７０】したがって、本実施の形態での構成によれば、埋込情報Ｄ１を抽出するために必要な公開鍵情報ｋｐを秘密に管理する必要がなくなり、誰でも自由に埋込情報Ｄ１を抽出でき、その内容を確認することができる。また、不正なユーザによって埋込情報Ｄ１が破壊されたり、変更されたとしても、上述の秘密情報Ｄ３を用いて埋込情報Ｄ１を復元することができるため、原画像データＧの著作権を十分に保護することができ、埋込情報Ｄ１の信頼性と安全性を向上させることもできる。

【００７１】尚、本実施の形態での抽出装置２００において、更に、電子透かし抽出回路２０１により抽出された埋込情報Ｄ１と、電子透かし抽出回路２０３から抽出された埋込情報Ｄ１とを比較し、電子透かし画像データＧ’に埋め込まれている埋込情報Ｄ１が改竄されているか否かを検出するように構成してもよい。これにより、抽出装置２００に改竄検出機能を付加することができ、電子透かし画像データＧ’の著作権保護をより一層高めることができる。また、改竄検出の結果を表示部２０４に供給することによって、電子透かし画像データＧ’の正当性をユーザに視覚的に通知することもできる。

【００７２】また、抽出装置２００に付加する改竄検出機能としては、上述の機能構成のものに限らず、例えば、符号系列データＤ４の誤りが、誤り訂正復号回路２０２の訂正能力を超えた場合（すなわち、誤り訂正不能となる場合）に、埋込情報Ｄ１が改竄されたと検出するようにしてもよい。これにより、抽出装置２００に付加する改竄検出機能を、簡単に構成することができる。

【００７３】［埋込装置１００での埋込手法、及び抽出装置２００での抽出手法］図３～５を用いて、埋込装置１００に適用される埋込手法の一例と、抽出装置２００に適用される抽出手法の一例とについて具体的に説明する。

【００７４】（１）埋込方法

図３は、本実施の形態における埋込方法の手順を示したものである。

【００７５】ステップＳ４１１：先ず、埋込情報Ｄ１を、上述した公開情報埋込部に埋め込む。すなわち、電子透かし埋込回路１０１は、公開鍵情報ｋｐを用いて原画像データＧを操作し、原画像データＧに埋込情報Ｄ１を埋め込む。このとき、電子透かし埋込回路１０１は、所定の規則に従って、公開情報埋込部の画像データを操作する。上記の所定の規則とは、例えば、埋め込み対象となる変数を原画像データＧの画素の輝度値とした場合、原画像データＧの輝度の平均値（すなわち、全画素の輝度の平均値）Ｃと、図４に示すような、公開情報埋込部を構成するブロックの輝度の平均値C_{ij}（縦方向ｉ番目、横方向ｊ番目のブロックを公開情報埋込部としたときの該ブロックの輝度の平均値）との間に予め設定された規則である。ここでは、あるブロックに“１”を埋め込む場合、「$C \leqq C_{ij}$」となるように、そのブロックの輝度の平均値C_{ij}を操作する。また、あるブロックに“０”を埋め込む場合には、「$C > C_{ij}$」となるように、そのブロックの輝度の平均値C_{ij}を操作するものとする。したがって、上記図４において、公開情報埋込部となるブロックをＣ23及びＣ24とし、各ブロックに埋め込む埋込情報Ｄ１を｛１，０｝とした場合、電子透かし埋込回路１０１は、$C \leqq C_{23}$、$C > C_{24}$となるように、各ブロックの輝度の平均値C_{23}及びC_{24}を操作することになる。ここで、各ブロックの操作の大きさは、埋め込み強度によって決定される。尚、公開情報埋込部となるブロックの位置及び埋め込み強度は、上述したような一般のユーザに公開することのできる情報である。

【００７６】ステップＳ４１２～ステップＳ４１９：次に、秘密情報Ｄ３を埋め込む。例えば、情報の埋込の対象となる変数を、原画像データＧの画素の輝度値とした場合、次のようなステップＳ４１２～ステップＳ４１９の処理が実行される。

【００７７】先ず、判定値抽出回路１０２は、原画像データＧの輝度の平均値（以下、これを”Ｃ”で示す）を求める（ステップＳ４１２）。次に、判定値抽出回路１０２は、上記図５に示すように、原画像データＧを複数のブロック（ここでは、４×４の１６ブロック）に分割し（ステップＳ４１３）、それぞれのブロック毎の輝度の平均値C_{ij}を求める（ステップＳ４１４）。そして、各ブロックの処理順を定める。ここでは、その処理順を、C_{11}，C_{12}，C_{13}，C_{14}，C_{21}，C_{22}，・・・，C_{43}，C_{44}のブロックの順番とする。次に、判定値抽出回路１０２は、埋込情報Ｄ１の埋め込まれたブロック（すなわち、公開情報埋込部）を判別する（ステップＳ４１５）。ここで、公開情報埋込部の各ブロックには、ステップＳ４１１にて説明した規則に従って埋込情報Ｄ１が埋め込まれている。次に、判定値抽出回路１０２は、秘密情報Ｄ３を埋め込むブロック（すなわち、秘密情報埋込部）を決定し、埋込情報Ｄ１も秘密情報Ｄ３も埋め込まないブロック（すなわち、無情報埋込部）を決定する（ステップＳ４１６）。ここでは、上記図４において、

秘密情報埋込部を、C_{31}，C_{32}，C_{33}，C_{34}，C_{41}，C_{42}，C_{43}，C_{44}のブロックとし、無情報埋込部を、C_{11}，C_{12}，C_{13}，C_{14}，C_{21}，C_{22}のブロックとする。そして、判定値抽出回路１０２は、ステップＳ４１６にて決定した公開情報埋込部と無情報埋込部に対して、所定の判定処理を行い、データＤ２を検出する（ステップＳ４１７）。例えば、判定値抽出回路１０２は、各ブロックの輝度の平均値C_{ij}に対して、「$C \leqq C_{ij}$」のときC_{ij}＝“１”、「$C > C_{ij}$」のときC_{ij}＝“０”とする判定処理を行い、所定の順番に従って、各ブロックから“１”又は“０”を検出する。この検出結果がデータＤ２となる。

【００７８】尚、ここでは、公開情報埋込部に埋込情報Ｄ１を埋め込む規則と、公開情報埋込部と無情報埋込部からデータＤ２を検出する規則とを、同じ規則（すなわち、「$C \leqq C_{ij}$」のときC_{ij}＝“１”、「$C > C_{ij}$」のときC_{ij}＝“０”とする）としたが、これに限られるものではない。これらの規則の間に所定の関係（すなわち、データＤ２の一部が埋込情報Ｄ１と１対１に対応する関係）が成り立つのであれば、これらを全く逆の規則としてもよい。

【００７９】上述のようにして、判定値抽出回路１０２において、公開情報埋込部と無情報埋込部の各ブロックから所定の規則に従って検出されたデータＤ２は、誤り訂正符号化回路１０３に供給される。誤り訂正符号化回路１０３は、判定値抽出回路１０２からのデータＤ２を誤り訂正符号化し、パリティデータＤ３を生成する（ステップＳ４１８）。ここでは、このパリティデータＤ３が上述の秘密情報となる。そして、電子透かし埋込回路１０４は、秘密鍵情報ｋｓに基づいて、誤り訂正符号化回路１０３にて生成されたパリティデータＤ３を、判定値抽出回路１０２により決定された（ステップＳ４１６参照）秘密情報埋込部に埋め込む（ステップＳ４１９）。

【００８０】ここで、電子透かし埋込回路１０４にて用いられる秘密鍵情報ｋｓは、少なくとも秘密情報埋込部の位置が含まれる。この秘密鍵情報ｋｓは、公開鍵情報ｋｐと異なり一般に公開されることはない。ステップＳ４１９では、秘密情報Ｄ３の埋込規則を、秘密情報埋込部及び無情報埋込部からデータＤ２を検出する規則と同じとする。これにより、抽出装置２００では、単一の規則により秘密情報Ｄ３とデータＤ２を抽出することができ、処理を簡略化することができる。また、秘密情報Ｄ３の埋込規則を、公開情報Ｄ１の埋込規則と同じとすることにより、抽出装置２００側の処理を更に簡略化することができる。

【００８１】尚、ステップＳ４１９での埋め込み規則は、上述の規則と異なった規則であってもよい。例えば、上記図５において、無情報埋込部をC_{11}～C_{22}のブロックとし、公開情報埋込部をC_{23}，C_{24}のブロックとし、秘密情報埋込部をC_{31}～C_{44}のブロックとした場合、電子透かし埋込回路１０４は、「$C \leqq C_{ij}$」となるようにそのブロックの輝度の平均値C_{ij}を操作することにより“０”を埋め込む。また、「$C > C_{ij}$」となるようにそのブロックの輝度の平均値C_{ij}を操作することにより“１”を埋め込む。

【００８２】また、誤り訂正符号化回路１０３にて用いる誤り訂正符号化方法としては、例えば、（１５，７，５）のＢＣＨ符号（今井秀樹著、電子情報通信学会発行：“符号理論”７．１節参照）を採用するものとしてよい。この場合、符号長がC_{12}～C_{44}のブロックから検出される“１５”、情報長がC_{12}～C_{24}のブロックから検出される“７”、最小距離が“５”となる誤り訂正符号が構成することができる。これにより、C_{31}～C_{44}の各ブロックには、C_{12}～C_{24}の各ブロックから検出されたデータに基づいて算出された８ビットのパリティデータＤ３が埋め込まれることになる。

【００８３】さらに、誤り訂正符号化回路１０３にて用いる誤り訂正符号化方法としては、上述の（１５，７，５）のＢＣＨ符号に限られず、例えば、各ブロックを更に細かく分割し、公開情報埋込部と秘密情報埋込部の少なくとも一方を大きくすることによって、誤り訂正能力をより向上させた誤り訂正符号化方法を採用するようにしてもよい。

【００８４】（２）抽出手法

図５は、本実施の形態における抽出方法の手順を示したものである。

【００８５】ステップＳ４２１：まず、抽出方法に必要な情報、すなわち公開情報埋込部として決定されたブロック（ここでは、C_{23}及びC_{24}の各ブロックとする）の位置、及び埋込情報Ｄ１の埋込規則と抽出規則は、公開鍵情報ｋｐの一部として一般に公開されている。そこで、電子透かし抽出回路２０１は、埋込情報Ｄ１が埋め込まれたディジタル画像データ（すなわち、電子透かし画像データＧ’）を受け取り、上記図４に示したような複数のブロック（ここでは、４×４の１６ブロック）に分割し、各ブロック毎の輝度の平均値C_{ij}を求める。

【００８６】ステップＳ４２２：次に、電子透かし抽出回路２０１は、電子透かし画像データＧ’の輝度の平均値（すなわち、全画素の輝度の平均値）Ｃを求める。ここで、この平均値Ｃを、公開鍵情報ｋｐの一部として公開するようにしてもよい。

【００８７】ステップＳ４２３：次に、電子透かし抽出回路２０１は、上記図４に示す全てのブロックに対して所定の規則に基づいた判定処理を行い、符号系列データＤ４を生成する。ここでの所定の規則とは、上述した（１）埋込方法と対応するものであり、例えば、各ブロックの輝度の平均値C_{ij}に対して、「$C \leqq C_{ij}$」のときC_{ij}＝“１”、「$C > C_{ij}$」のときC_{ij}＝“０”とする規則である。各ブロックの判定結果は、予め定められた

ブロックの順番に従って並べられ、符号系列データＤ４となる。この符号系列データＤ４が、誤り訂正復号回路２０２に供給されることになる。

【００８８】ステップＳ４２４：誤り訂正復号回路２０２は、電子透かし抽出回路２０１からの符号系列データＤ４を用いて、上述した（１）埋込方法の誤り訂正符号化方法に対応する誤り訂正復号を行う。この復号された符号系列データＤ４は、訂正系列データＤ５として電子透かし抽出回路２０３に供給される。ここで、例えば、公開情報埋込部であるC_{23}及びC_{24}の各ブロックに存在する情報に対して破壊、或いは画素値の変更や切取り等が行われていた場合、上記の符号系列データＤ４には、少なくとも２ビットの誤りを含むことになる。しかしながら、符号系列データＤ４は、所定の方式（例えば、（１５，７，５）のＢＣＨ符号）に基づいて、誤り訂正符号化されているデータであるため、この方式に対応する復号処理を施せば、破壊や変更された少なくとも２ビットのデータを訂正し、復元することができる。したがって、この結果、誤り訂正復号回路３０２は、復元された符号系列データＤ４（訂正系列データＤ５）を得ることができる。

【００８９】ステップＳ４２５：電子透かし抽出回路２０３は、誤り訂正復号回路２０２からの訂正系列データＤ５の中から、公開埋込情報Ｄ１（或いは、公開埋込情報Ｄ１と１対１に対応するデータ）を検出することによって、公開埋込情報Ｄ１（例えば、｛１，０｝）を取得する。この結果、例え破壊されても、復元可能な範囲であれば、常に正しい公開埋込情報Ｄ１が抽出装置２００にて認識されることになる。ここで、公開埋込情報Ｄ１は、公開鍵情報ｋｐ（例えば、公開情報埋込部の位置）に基づいて、訂正系列データＤ５の中から検出される。

【００９０】尚、上述した（２）抽出方法では、少なくとも２ビットの誤りを訂正することのできる誤り訂正符号を抽出し、それを復号するものとしたが、これに限らず、例えば、ブロックの分割を更に細かくし、パリティデータの埋め込める秘密情報埋込部の領域を大きくすることで、２つ以上の誤りの訂正と、公開埋込情報Ｄ１以外に生じた誤りの訂正とに対応させることもできる。

【００９１】［（１）埋込手法、（２）抽出手法の応用例］上述した（１）埋込方法と（２）抽出方法を応用することにより、埋込情報の耐性の向上、抽出情報の誤り訂正能力の向上、原画像の画質劣化の抑制等、様々な効果をもたらす埋込方法と抽出方法を構成することもできる。以下、図６及び図７を用いて、第１の実施の形態の変形例１～６を説明する。尚、図６及び図７において、上記図１での同様の構成或いは機能を有する処理部については同一の符号を付し、その詳細な説明を省略する。

【００９２】（例１）：上記図１に示した埋込装置１００では、埋込情報Ｄ１を符号化することなく原画像データＧに埋め込む構成について説明したが、これに限らず、例えば、埋込情報Ｄ１を誤り訂正符号化処理や、暗号化処理等の一方向性関数的な演算により符号化してもよい。

【００９３】具体的には例えば、上記図１の埋込装置１００において、図６（ａ）に示すように、誤り訂正符号化回路１０７を新たに設ける。この場合、誤り訂正符号化回路１０７は、上述の埋込情報Ｄ１自体を誤り訂正符号化する。或いは、上記図１の埋込装置１００において、上記図６（ｂ）に示すように、公開鍵暗号方式の機能を有する暗号化回路１０８を新たに設けることも可能である。この場合、暗号化回路１０８は、上述の埋込情報Ｄ１自体を、秘密鍵を用いて公開鍵暗号化する。さらに、上記図１の埋込装置１００において、上記図６（ａ）に示したような誤り訂正符号化回路１０７、及び同図（ｂ）に示したような暗号化回路１０８を組み合わせた構成を新たに設けることも可能である。この場合、上述の埋込情報Ｄ１には、誤り訂正符号化と暗号化が交互に施される。

【００９４】ここで、上記の一方向性関数とは、関数ｙ＝ｆ（ｘ）において、ｘからｙを求めることは容易であるが、逆にｙからｘを求めることの困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散的対数等が一方向性関数としてよく用いられる。このような一方向関数を用いて符号化する構成とする場合、埋込装置１００の電子透かし埋込回路１０１には、誤り訂正符号化回路１０７により誤り訂正符号化された埋込情報Ｄ１（すなわち、符号化埋込情報Ｄ１’）、暗号化回路１０８により暗号化された埋込情報Ｄ１（すなわち、暗号化埋込情報Ｄ１”）、及び誤り訂正符号化回路１０７と暗号化回路１０８の組合せにより符号化された埋込情報Ｄ１の何れかの情報が、上記図１での埋込情報Ｄ１の代わりに供給されることになる。このような構成とすることで、埋込情報Ｄ１の耐性、埋込情報Ｄ１の誤りを訂正する能力、埋込情報Ｄ１の安全性と信頼性を向上させることができる。

【００９５】尚、上記図１の埋込装置１００を、上記図６（ａ）の構成、同図（ｂ）の構成、或いはその両方を組み合わせた構成とした場合、抽出装置２００を、その構成に対応した構成とすれば、抽出装置２００は、埋込装置１００にて符号化された埋込情報Ｄ１を抽出し、復号することができる。

【００９６】（例２）：上述した（１）埋込方法では、埋込情報Ｄ１を符号化することなく、原画像データＧの公開情報埋込部に埋め込むようにしたが、これに限らず、例えば、上記図６（ａ）に示したような構成を有する埋込装置１００のように、埋込情報Ｄ１を誤り訂正符号化したデータ（すなわち、埋込情報Ｄ１’）を、原画像データＧの公開情報埋込部に埋め込むようにしてもよい。この場合、抽出装置２００は、公開情報埋込部とその他の部分から検出された情報を復号し、誤りを検出

し、そして訂正する。このとき、公開情報埋込部から検出された情報（すなわち、埋込情報Ｄ１’）に誤りが検出された場合、抽出装置２００において更に、その情報を復号し、消失訂正するように構成することもできる。これにより、誤り訂正能力をより一層向上させることができる。また、埋込情報Ｄ１の復元をする能力をより一層向上させることもできるため、埋め込み情報の耐性を更に向上させることができる。

【００９７】（例３）：上述した（１）埋込方法において、公開情報埋込部及び秘密情報埋込部とするブロックの選択は任意であり、ランダムに選択可能であるが、その選択を次のようにしてもよい。

【００９８】具体的には、まず、C_{ij}の値が平均値Ｃに近いものは、圧縮や種々の変形によって値が変化しやすいため、情報の埋込時には「Ｃ≦C_{ij}」であっても、情報の抽出時には「Ｃ＞C_{ij}」となることが考えられる。このようなブロックが無情報埋込部として選択されると、抽出時にデータＤ２が誤って検出される場合がある。そこで、例えば、耐性が弱い、すなわちC_{ij}の値が平均値Ｃに近いブロックを、埋込情報Ｄ１又は秘密情報Ｄ３を埋め込むブロックとし、それらのブロックを操作して、予めある程度の強度を持たせるようにする。これにより、圧縮や種々の変形に耐性のある電子透かしの埋込方法を実現できる。また、この場合、C_{ij}の値が平均値Ｃに近いブロックに対して、「Ｃ≦C_{ij}」又は「Ｃ＞C_{ij}」となるような操作を加えることになるため、その分変化量をほぼ半分程度に抑えることができ、したがって、画質劣化を小さくすることができる（例えば、平均値Ｃよりも非常に大きい値C_{ij}を有するブロックに対して、「Ｃ＞C_{ij}」となるような操作を加える必要がある場合、このときの画質劣化は大きい）。

【００９９】また、無情報埋込部となるブロックの選択については、埋込装置１００の構成を、例えば、図７に示すように、判定値抽出回路１０２を電子透かし埋込回路１０１の前段に設け、判定値抽出回路１０２により、原画像データＧの各ブロックの判定値を予め抽出し、この判定値に基づいて、各情報を埋め込むブロックを決定するようにしてもよい。これにより、C_{ij}の値が平均値Ｃに近くないブロックを無情報埋込部として選択することができる。

【０１００】上述のようなブロック選択のための構成により、電子透かし画像の画質劣化を更に小さく、且つ埋込情報Ｄ１の耐性をより一層強化することができる。

【０１０１】（例４）：上述した（１）埋込方法では、ブロックの順番を任意に定めることができるが、次のような構成によってブロックの順番を定め、秘密情報Ｄ３を埋め込むようにしてもよい。例えば、上記図７の埋込装置１００において、原画像データＧの各ブロックの輝度の平均値C_{ij}を予め判定した後、その原画像データＧの各ブロックの判定値自体が、埋込情報Ｄ１を復元するための秘密情報となるように各ブロックの順番を定める。この場合、情報の埋込を行う（すなわち、画像データに操作を加える）ブロックの数が略最小距離の数となり、原画像データＧや埋込情報Ｄ１に係わらず略一定となる。

【０１０２】具体的には、上記図７の構成において、先ず、判定値抽出回路１０２は、原画像データＧのブロックの値を判定した後、平均値Ｃに近くないC_{ij}のブロックを無情報埋込部のブロックとして、任意にブロックの順番を定める。次に、判定値抽出回路１０２は、平均値Ｃに近いC_{ij}のブロックの一部を公開情報埋込部のブロックとして、任意にブロックの順番を定める。そして、誤り訂正符号化回路１０３は、判定値抽出回路１０２にて定められた順番に従って並べられた公開情報埋込部のブロックの判定値と、無情報埋込部のブロックの判定値とを、データＤ６として誤り訂正符号化する。その後、誤り訂正符号化回路１０３は、データＤ６のパリティデータＤ３を秘密情報として電子透かし埋込回路１０４に供給する。電子透かし埋込回路１０４は、秘密情報埋込部（平均値Ｃに近いC_{ij}のブロックの一部）の判定値を用いて、各ブロックの順番をパリティデータＤ３を構成する順番となるように定める。

【０１０３】したがって、上述のような構成とすることにより、原画像データＧを実際に操作することなく、秘密情報Ｄ３の埋め込みを行うことができるため、操作を加えるブロックの数を小さく、且つ平均的にすることができる。また、原画像データＧの画質に与える影響をより一層抑制することもできる。

【０１０４】（例５）：上述した（１）埋込方法では、原画像データＧから検出されたデータＤ２を１つのデータとして符号化する（すなわち、データＤ２を誤り訂正符号化する）ようにしたが、これに限らず、例えば、原画像データＧから検出されたデータＤ２を複数の部分データに分割し、各部分データ毎に、又は重複を許す部分データ毎に、誤り訂正符号化するようにしてもよい。

【０１０５】（例６）：上述した（１）埋込方法では、原画像データＧを複数のブロックに分割した後、各ブロックの輝度の平均値を操作することにより、埋込情報Ｄ１及び秘密情報Ｄ３の埋め込みを行うようにしたが、これに限られるものではない。また、上述した（１）埋込方法では、誤り訂正符号化方法として、（１５，７，５）のＢＣＨ符号化を採用するようにしたが、これに限られるものでもない。例えば、情報の埋め込みについては、ウェーブレット変換や離散コサイン変換等の周波数変換方式を用いて、１つ以上のブロックを周波数変換し、所定の周波数領域に対して情報の埋め込みを行うようにしてもよい。或いは、フーリエ変換を用いてこれを行うようにしてもよい。或いは、画像の画素を操作することによって、空間領域に対する情報の埋め込みを行うようにしてもよい。尚、周波数変換方式を用いて埋込処

理を行う場合、公開情報Ｄ１と秘密情報Ｄ３とを異なる周波数領域に対して埋め込むようにしてもよい。

【０１０６】具体的には、例えば、フーリエ変換を用いる場合、原画像データＧ全体をフーリエ変換し、その変換値の中から耐性等に応じて、いくつかの情報を埋め込む部分の候補を決定し、その決定した部分の一部を公開情報埋込部（公開鍵情報ｋｐに基づく情報埋め込み領域）とし、その他の部分を秘密情報埋込部（秘密鍵情報ｋｓに基づく情報埋め込み領域）、或いは無情報埋込部（何も情報を埋め込まない領域）とすれば、本実施の形態での（１）埋込方法と同様の原理を応用することができる。このとき、上述の複数の異なる埋め込み方法を組合せ、埋込情報Ｄ１及び秘密情報Ｄ３を原画像データＧに埋め込むように構成してもよい。

【０１０７】また、誤り訂正符号化方法としては、例えば、他のブロック符号化方式や、畳み込み符号化（木符号化）方式等、種々の誤り訂正符号化方式を採用することができる。

【０１０８】また、埋め込み対象となるディジタルデータについても、ディジタル画像データに限らず、動画像データ、テキストデータ、音声データ、グラフィックスデータ、プログラムデータ等、種々のディジタルデータを対象とすることができ、何れのディジタルデータに対しても、本実施の形態での埋込方法を応用することができ、また、埋込情報Ｄ１の埋め込みと抽出に必要な鍵情報を、一般に公開することができる。

【０１０９】上述したような、本実施の形態の変形例１～６によれば、埋め込み情報の耐性の向上、埋め込み情報を復元する能力（即ち、誤り訂正能力）の向上、原画像の画質劣化の抑制等、様々な効果をもたらす埋込方法と抽出方法とを提供することができる。

【０１１０】（第２の実施の形態）本実施の形態では、上述した第１の実施の形態における埋込装置１００と抽出装置２００を用いて構成されるシステムを、例えば、図８に示すような構成のシステムに適用する。このシステムは、公衆回線、インターネット、イーサネット等からなるネットワーク３００を用いて構成されるシステムであって、例えば、静止画像データ、動画像データ、音声データ、テキストデータ、グラフィックスデータ、プログラムデータ等のディジタルデータを配布したり、売買したりするディジタル情報配布システムや、電子商取引システム等に適用されるものである。以下、本実施の形態でのシステムについて具体的に説明する。

【０１１１】尚、上記図８に示す本実施の形態でのシステムにおいて、第１の実施の形態でのシステムと同様の構成或いは機能を有する部分については同一の符号を付し、その詳細な説明を省略する。

【０１１２】先ず、上述した第１の実施の形態と同様にして、埋込装置１００は、公開鍵情報ｋｐに基づいて、埋込情報Ｄ１を原画像データＧに埋めこむ。次に、埋込装置１００は、埋込情報Ｄ１を復元するために必要な秘密情報（第１の実施の形態では、パリティデータＤ３）を、原画像データＧに埋めこむ。そして、埋込装置１００は、埋込情報Ｄ１及び秘密情報を埋め込んだ電子透かし画像データＧ’を、所定の手順（例えば、ディジタル情報配布システムや電子商取引システムに基づく手順）に従って、ネットワーク３００に対して送出する。

【０１１３】ここで、埋込装置１００にて用いられる公開鍵情報ｋｐは、一般に公開された情報であり、埋込装置１００と抽出装置２００との間で秘密に管理する必要がなく、また、埋込装置１００と抽出装置２００との間のネットワーク３００を介して自由に送受信できる情報である。ここでは、公開鍵情報ｋｐは、埋込装置１００にて電子透かし画像データＧ’に付加されて、ネットワーク３００対して送出されるものとする。

【０１１４】一方、抽出装置２００は、公開鍵情報ｋｐに基づいて、ネットワーク３００を介して供給された電子透かし画像データＧ’から、埋込情報Ｄ１を抽出する。このとき、上述した第１の実施の形態と同様に、抽出装置２００は、電子透かし画像データＧ’に埋め込まれた秘密情報を用いて、埋込情報Ｄ１を復元することもできる。また、公開鍵情報ｋｐに基づいて抽出された埋込情報Ｄ１と、秘密情報を用いて復元された埋込情報Ｄ１とを比較することにより、電子透かし画像データＧ’に対する改竄を検出することもできる。

【０１１５】したがって、本実施の形態によれば、上述した第１の実施の形態と同様に、埋込情報Ｄ１を埋め込む際に必要な公開鍵情報ｋｐを秘密に管理する必要がなく、一般に自由に公開することができる。これにより、公開鍵情報ｋｐの管理が容易で、誰でも自由に埋込情報Ｄ１の内容を確認することのできるシステムを構築することができる。また、原画像データＧには、埋込情報Ｄ１を復元するための秘密情報Ｄ３を埋め込むため、原画像データＧの著作権を十分に保護することもできる。

【０１１６】尚、上述した第２の実施の形態において、埋込装置１００は、所定のファイルフォーマットに従って、公開鍵情報ｋｐを電子透かし画像データＧ’に付加するようになされているものとする。例えば、画像データ部と画像ヘッダ部を含む画像ファイルフォーマットを採用する場合、電子透かし画像データＧ’を画像データ部に格納し、公開鍵情報ｋｐを画像ヘッダ部に属性情報として格納する。このようなファイルフォーマットの構成については、後述する第４の実施の形態において詳細に説明する。

【０１１７】また、上述した第２の実施の形態では、電子透かし画像データＧ’に公開鍵情報ｋｐを付加して、ネットワーク３００に対して送出するものとしたが、これに限らず、例えば、電子透かし画像データＧ’と公開鍵情報ｋｐをそれぞれ別情報として、それぞれで送出するようにしてもよい。

【０１１８】また、上述した第２の実施の形態において、埋込装置１００から送出された公開鍵情報ｋｐの正当性を検査するために、送信者自身の公開鍵暗号方式に基づくディジタル署名を公開鍵情報ｋｐに対して施すような構成をとるようにしてもよい。この場合においても、公開鍵情報ｋｐの秘密通信は必要ない。これにより、埋込情報Ｄ１の破壊や変更が難しくなり、安全性と信頼性とをより一層向上させたシステムを提供することができる。

【０１１９】（第３の実施の形態）本実施の形態では、上述した第２の実施の形態における埋込装置１００と抽出装置２００を用いて構成されるシステムを、例えば、図９に示すような構成のシステムに適用する。このシステムは、上述した第２の実施の形態でのシステム構成（上記図８参照）に加えて、鍵管理局５００を更に含んだ構成としている。以下、本実施の形態でのシステムについて具体的に説明する。

【０１２０】尚、上記図９に示す本実施の形態でのシステムにおいて、第１又は第２の実施の形態でのシステムと同様の構成或いは機能を有する部分については同一の符号を付し、その詳細な説明を省略する。

【０１２１】まず、上記図９のシステムは、公衆回線、インターネット、イーサネット等からなる鍵管理局５００を含んだネットワーク３００を用いて構成されるシステムであって、例えば、静止画像データ、動画像データ、音声データ、テキストデータ、グラフィックスデータ、プログラムデータなどのディジタルデータを配布したり、売買したりするディジタル情報配布システムや、電子商取引システムに適用されるものである。

【０１２２】そこで、本システムにおいては、上述した第２の実施の形態と同様にして、埋込装置１００から送出された公開鍵情報ｋｐの正当性を検査するために、送信者自身の公開鍵暗号方式に基づくディジタル署名を公開鍵情報ｋｐに対して施すこともできるが、ここでは、鍵管理局５００の公開鍵暗号方式に基づくディジタル署名を、埋込装置１００から送出された公開鍵情報ｋｐに対して施すように構成する。すなわち、鍵管理局５００が、公開鍵情報ｋｐの正当性を保証するように構成する。これにより、埋込情報Ｄ１の破壊や変更が難しくなり、安全性と信頼性とをより一層向上させたシステムを提供することができる。

【０１２３】上述のような構成をとることで、鍵管理局５００は、公開暗号方式における認証局と同様の機能を有することになる。ここで、上記の”認証局”とは、公開暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関のことを言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成して発行する。これにより、あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、その証明書を認証局の公開鍵を用いて検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであること）を認証する。このような認証局を運営している組織としては、「ＶｅｒｉＳｉｇｎ」やＣｙｂｅｒＴｒｕｓｔ」等の企業がよく知られている。

【０１２４】したがって、鍵管理局５００は、埋込装置１００からネットワーク３００に対して送出された公開鍵情報ｋｐに対して、自分のディジタル署名を施し、これを公開鍵情報ｋｐ’として、抽出装置２００に与えることになる。そして、抽出装置２００は、鍵管理局３００からの公開鍵情報ｋｐ’を用いて、埋込装置１００からの電子透かし画像データＧ’から埋込情報Ｄ１を抽出する。

【０１２５】尚、上述した第３の実施の形態では、鍵管理局５００にて署名が施された公開鍵情報ｋｐ’を、抽出装置２００に与えるようにしたが、例えば、埋込装置１００に対して与えるようにしてもよい。この場合、埋込装置１００は、鍵管理局５００からの公開鍵情報ｋｐ’を、電子透かし画像データＧ’と共に、抽出装置３００にネットワーク３００を介して与えるようにする。

【０１２６】また、上述した第３の実施の形態において、鍵管理局５００を、例えば、不正配布の検査センター等として機能させるようにしてもよい。また、上述した第３の実施の形態において、埋込装置１００から送出される電子透かし画像データＧ’を、例えば、暗号化されたデータとするようにしてもよい。

【０１２７】（第４の実施の形態）本実施の形態では、上述した第１～第３の実施の形態にける埋込装置１００が、電子透かし画像データＧ’と公開鍵情報ｋｐをネットワーク３００に対して送出する際の、ファイルフォーマットとして、例えば、次のようなファイルフォーマットを採用する。

【０１２８】まず、通常の、一般的な画像ファイルフォーマットは、例えば、図１０に示すようなフォーマット６００で示される。これにより、埋込装置１００は、ファイルフォーマット６００に従って、送付する電子透かし画像データＧ’を画像データ部６０２に格納し、それに対する公開鍵情報ｋｐを画像ヘッダ部６０１に格納する。一方、ＦｌａｓｈＰｉｘＴＭ（”ＦｌａｓｈＰｉｘ”は米国ＥａｓｔｍａｎＫｏｄａｋ社の登録商標）ファイルフォーマットでは、詳細は後述するが、公開鍵情報ｋｐと電子透かし画像データＧ’を、各階層のデータとして格納することができるようになされている。また、公開鍵情報ｋｐ等を属性情報として、プロパティセットの中に格納しておくこともできるようになされている。以下、一般的なファイルフォーマット、及びＦｌａｓｈＰｉｘＴＭファイルフォーマットについて具体的に説明する。

【０１２９】［一般的な画像ファイルフォーマット］－

般的な画像ファイルフォーマットは、上記図１０に示したように、画像ファイルが画像ヘッダ部６０１と画像データ部６０２に分けられた構造としている。画像ヘッダ部６０１には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。上記図１０の例では、画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置のオフセット、及びカラーパレット、そして、公開鍵情報ｋｐ等の画像属性情報が格納されている。一方、画像データ部６０２には、画像データ自体が格納されている。このような画像ファイルフォーマットの代表的な例としては、Ｍｉｃｒｏｓｏｆｔ社のＢＭＰフォーマットや、Ｃｏｍｐｕｓｅｒｖｅ社のＧＩＦフォーマット等が広く普及している。

【０１３０】［ＦｌａｓｈＰｉｘ TMファイルフォーマット］以下に説明するＦｌａｓｈＰｉｘTMファイルフォーマットでは、上記図１０に示した画像ヘッダ部６０１に格納される画像属性情報、及び画像データ部６０２に格納される画像データを、階層構造化して画像ファイル内に格納するようになされている。この階層構造化された画像フィルフォーマットとしては、例えば、図１１や図１２に示すようなフォーマットがある。以下、これらの図１１及び図１２を用いて、ＦｌａｓｈＰｉｘTMファイルフォーマットについて説明する。

【０１３１】まず、ファイル内の各プロパティやデータに対しては、ＭＳ－ＤＯＳのディレクトリとファイルに相当するストレージとストリームによってアクセスする。上記図１１及び図１２では、影付きブロックがストレージを示し、影無しブロックがストリームを示しており、画像データや画像属性情報（公開鍵情報ｋｐ等を含む情報）は、ストリーム部分に格納される。また、上記図１２は、画像データが異なる解像度で階層化されて格納される様子を示しており、それぞれの解像度の画像を、ここでは”Ｓｕｂｉｍａｇｅ”と呼び、これらを”Resolution０，１，・・・，ｎ”で示している。そして、それぞれの解像度の画像に対して、対象画像データを読み出すために必要な情報が”Subimage Header ”７０８に格納され、画像データが”Subimagedata”７０７に格納される。

【０１３２】上記図１１及び図１２に示す”Property Set”（プロパティセット）とは、画像属性情報を、その使用目的や内容に応じて分類して定義したものであり、このような”Property Set”としては、”Summary info.Property Set ”７０１、”Image info.Property Set ”７０４、”Image Content Property Set”７０３、”Extention list Property Set ”７０５等がある。

【０１３３】上記図１１及び図１２に示す”Summary info.Property Set ”７０１は、ＦｌａｓｈＰｉｘ特有のものではなく、Ｍｉｃｒｏｓｏｆｔ社のストラクチャードストレージでは必須のものであり、画像ファイルのタイトル名、題名、著者、サムネール画像等が格納される。上記図１１及び図１２に示す”Comp Obj.Stream ”７０２には、記録部（Strage）に関する一般的な情報が格納される。上記図１１に示す”Image Content Property Set”７０３には、画像データの格納方法が記述される。例えば、図１３に示すように、画像データの階層数、最大解像度の画像についての幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、或いはＪＰＥＧ圧縮方式を用いる際の量子化テーブル・ハフマンテーブルの定義等が記述される。上記図１１及び図１２に示す”Extention list Property Set ”７０５は、ＦｌａｓｈＰｉｘの基本仕様に含まれない情報を追加格納する際に仕様する領域である。したがって、例えば、上述した第１～第３の実施の形態における公開鍵情報ｋｐは、この”Extention list Property Set ”７０５に格納されることになる。上記図１１に示す”ICC Profile ”７０６には、ICC（International ColorConsortium）において規定される色空間変換のための変換プロファイルが記述される。

【０１３４】上記図１１に示す”Image info.Property Set ”７０４には、画像データを使用する際に利用できる次の（１）～（９）に示すような情報、すなわち、その画像がどのようにして取り込まれ、どのように利用可能であるか等の情報が格納される。

（１）ディジタルデータの取り込み方法、或いは生成方法に関する情報

（２）著作権に関する情報

（３）画像の内容（画像中に存在する人物や場所等）に関する情報

（４）撮影に使用されたカメラに関する情報

（５）撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無等）の情報

（６）ディジタルカメラ特有の解像度やモザイクフィルタに関する情報

（７）フィルムのメーカ名、製品名、種類（ネガ／ポジ、カラー／白黒等）等の情報

（８）オリジナル画像が書物や印刷物である場合の、その種類やサイズ等に関する情報

（９）スキャン画像の場合の、そのスキャンに使用したスキャナやソフト、操作した人等に関する情報

【０１３５】上記図１２に示す”FlashPix Image View Object”は、画像を表示する際に用いるビューイングパラメータと画像データを合わせて格納する画像ファイルである。ここでのビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリング等の処理を、画像表示の際に適切にするために記憶しておく処理係数を示す。

【０１３６】上記図１２に示す”Global Property set”８０１には、ロックされている属性リストが記述され、例えば、最大画像のインデックスや、最大変更項目のインデックス、最終修正者に関する情報等が記述される。上記図１２に示す”Source FlashPix Image Object”８０２及び”Result FlashPix Image Object”８０３は、ＦｌａｓｈＰｉｘ画像データの実体である。”Source FlashPix Image Object”８０２は、必須であり、オリジナルの画像データが格納される。一方、”Result FlashPix Image Object”８０３は、オプションであり、ビューイングパラメータを使って画像処理した結果の画像データが格納される。上記図１２に示す”Source desc.Property Set”８０４及び”Result desc.Property Set”８０５は、上記の画像データの識別のためのプロパティセットであり、画像ＩＤ、変更禁止のプロパティセット、最終変更日時等の情報が格納される。上記図１２に示す”Transform Property Set”８０６は、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数等が格納される。

【０１３７】以上、本発明を適用した第１～第４の実施の形態について説明したが、本発明は、その精神、又は主要な特徴から逸脱することなく、他の様々な形で実施することができる。例えば、上述の実施の形態での埋込方法や抽出方法の一部或いは全てを、ソフトウェアの制御により処理することも可能である。例えば、上述した第１～第４の実施の形態での機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（すなわち、上記図１や図７の記憶媒体１０６、上記図２の記憶媒体２０６）を、それぞれの実施の形態での装置（すなわち、上記図１や図７の埋込装置１００、上記図２の抽出装置２００）に供給するように構成する。また、上述した各実施の形態での装置が具備する制御部（すなわち、上記図１や図７の制御回路１０５、上記図２の制御回路２０５）が、上記記憶媒体に格納されたプログラムコードを読み出して実行することによっても、上述した各実施の形態での機能を実現することができる。この場合、上記記憶媒体から読み出されたプログラムコード自体が、上述した各実施の形態での機能を実現することになり、そのプログラムコードを記憶した記憶媒体は、本発明を構成することとなる。上記プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。また、上述した各実施の形態での制御部上で稼動しているＯＳ（オペレーティングシステム）、或いはアプリケーションソフトウェア等が、上記記憶媒体から読み出されたプログラムコードの指示に基づき、実際の処理の一部或いは全てを実行することによっても、上述した各実施の形態での機能を実現することができる。さらに、上記記憶媒体から読み出されたプログラムコードが、上述した各実施の形態での制御部に接続された機能拡張ユニットの具備するメモリに書き込まれた後、その機能拡張ユニットに備わる制御部が、そのプログラムコードの指示に基づき、実際の処理の一部或いは全てを実行することによっても、上述した各実施の形態での機能を実現することができる。したがって、上述した第１～第４の各実施の形態では、あらゆる点で単なる例示に過ぎず、限定的に解釈してはならない。また、本発明の範囲は、特許請求の範囲によって示すものであって、明細書本文には何等拘束されない。さらに、特許請求の範囲の均等範囲に属する変形や変更は全て、本発明の範囲のものである。

【０１３８】

【発明の効果】以上説明したように本発明では、画像等のディジタルデータに対して、第１の情報（ディジタルデータの著作権を管理したり保護するための著作権情報等）と、該第１の情報を復元するための第２の情報とを埋め込む。

【０１３９】具体的には例えば、公開された鍵情報（公開鍵情報）を用いて、著作権情報等の埋込情報（第１の情報、所定の情報：電子透かし等）をディジタルデータに対して目に見えないように埋め込むと共に、この埋込情報を復元するための秘密情報（第２の情報：例えば、誤り符号化処理により生成する場合にはパリティデータ）をも、公開されていない鍵情報（秘密鍵情報）を用いて、目に見えないように埋め込む。このとき、埋込対象となっているディジタルデータにおいて、埋込情報が埋め込まれた領域（第１の領域）と、秘密情報が埋め込まれた領域（第２の領域）と、それらの情報が埋め込まれていない領域（第３の領域）との間には、所定の関係がある。したがって、このようにして埋込情報及び秘密情報が共に埋め込まれたディジタルデータを受け取った側では、上記の公開された鍵情報を用いて、そのディジタルデータから埋込情報（著作権情報等）を自由に抽出することができる。これにより、一般のユーザは、外部から入手したディジタルデータの著作権の内容や、その正当性を確認することができる。また、ディジタルデータに埋め込まれている埋込情報が、不正なユーザによって破壊或いは変更されていたとしても、その埋込情報と共に埋め込まれている秘密情報によって、該埋込情報を復元することができるため、ディジタルデータの著作権を十分に保護することができ、埋込情報の信頼性と安全性を共に向上させることもできる。

【０１４０】よって、本発明によれば、埋込情報の抽出に必要な鍵情報を秘密に管理することなく、一般のユーザによる自由な埋込情報の抽出と、ディジタルデータの著作権の保護とを同時に満たすことのできる著作権保護技術を提供することができる。このような本発明による技術は、特に、電子商取引システムやディジタル情報配

布システム等に適用して有効である。

【図面の簡単な説明】

【図１】第１の実施の形態において、本発明を適用したシステムの埋込装置の構成を示すブロック図である。

【図２】上記システムの抽出装置の構成を示すブロック図である。

【図３】上記埋込装置にて実行される埋込方法を説明するためのフローチャートである。

【図４】上記埋込方法において、原画像に対する情報の埋め込みを説明するための図である。

【図５】上記抽出装置にて実行される抽出方法を説明するためのフローチャートである。

【図６】上記埋込方法及び上記抽出方法の応用例１を説明するための図である。

【図７】上記埋込方法及び上記抽出方法の応用例３を説明するための図である。

【図８】第２の実施の形態における上記システムの構成を示すブロック図である。

【図９】第３の実施の形態における上記システムの構成を示すブロック図である。

【図１０】第４の実施の形態において、上記システムにて用いる画像ファイルフォーマットとしての、一般的な画像ファイルフォーマットを説明するための図である。

【図１１】上記システムにて用いる画像ファイルフォーマットとしての、階層構造化された画像ファイルフォーマットを説明するための図である。

【図１２】上記システムにて用いる画像ファイルフォーマットとしての、他の階層構造化された画像ファイルフォーマットを説明するための図である。

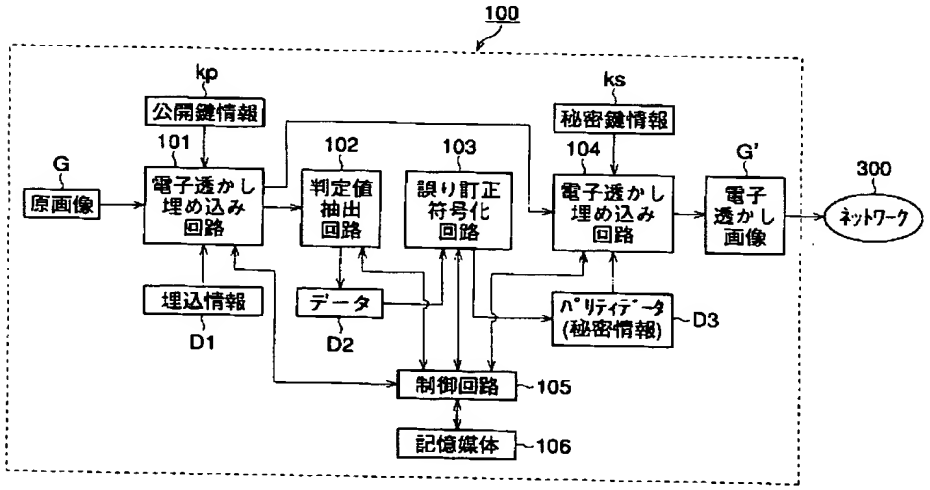
【図１３】上記階層構造化された画像ファイルフォーマットに格納される、画像データの格納方法についての情報の一例を説明するための図である。

【図１４】従来の電子透かし技術を用いたシステムの構成を示すブロック図である。

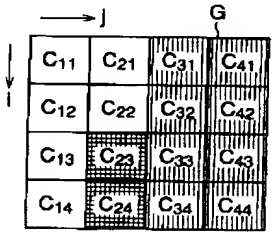
【符号の説明】

１００　埋込装置
１０１　電子透かし埋込回路
１０２　判定値抽出回路
１０３　誤り訂正符号化回路
１０４　電子透かし埋込回路
１０５　制御回路
１０６　記憶媒体
２００　抽出装置
２０１　電子透かし抽出回路
２０２　誤り訂正復号回路
２０３　電子透かし抽出回路
２０４　表示部
２０５　制御部
２０６　記憶媒体
３００　ネットワーク

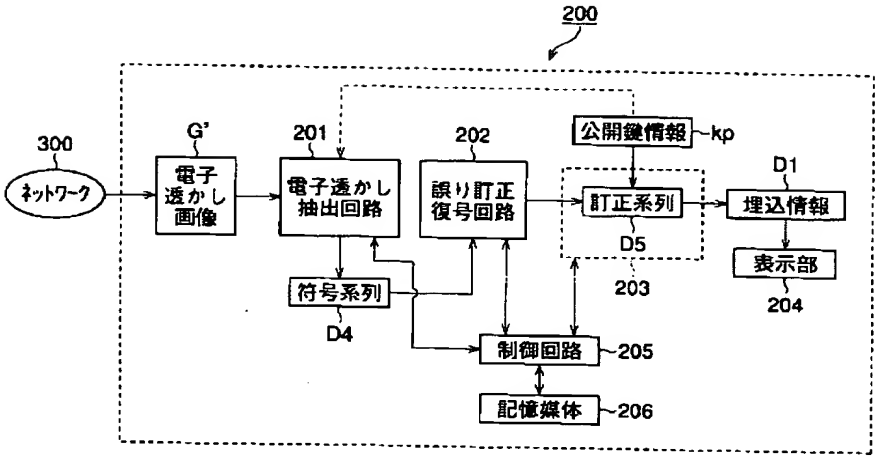
【図１】



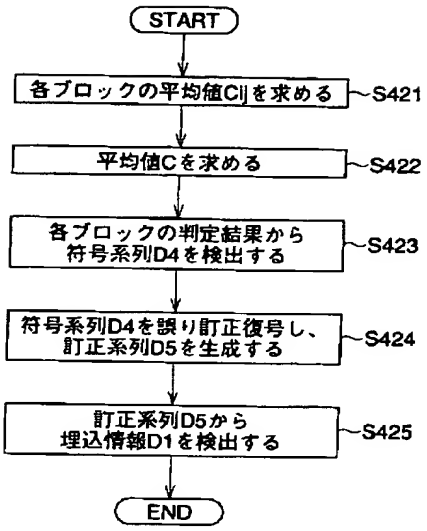
【図４】



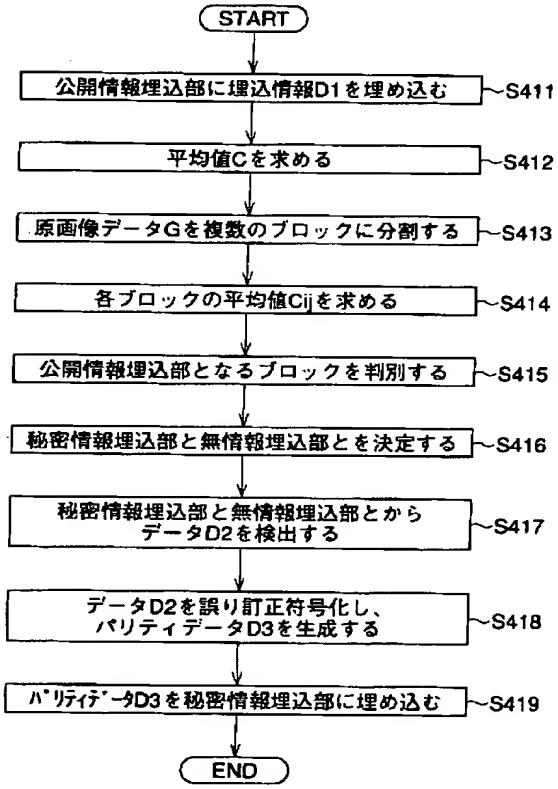
【図２】


200
300
ネットワーク
G'
電子透かし画像
201
電子透かし抽出回路
202
誤り訂正復号回路
公開鍵情報
kp
訂正系列
D5
203
D1
埋込情報
表示部
204
符号系列
D4
制御回路
205
記憶媒体
206

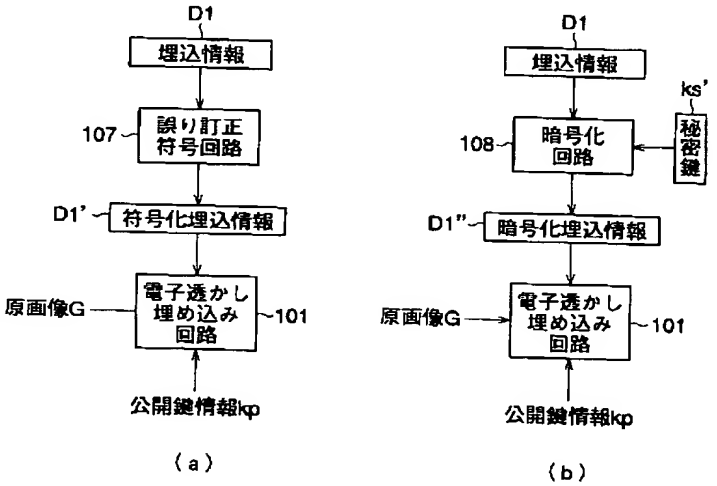
【図５】


START
各ブロックの平均値Cijを求める
S421
平均値Cを求める
S422
各ブロックの判定結果から符号系列D4を検出する
S423
符号系列D4を誤り訂正復号し、訂正系列D5を生成する
S424
訂正系列D5から埋込情報D1を検出する
S425
END

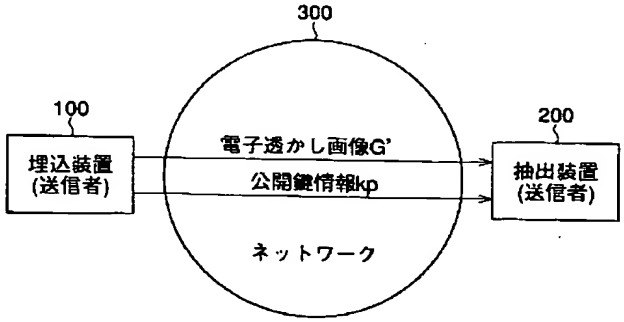
【図３】


START
公開情報埋込部に埋込情報D1を埋め込む
S411
平均値Cを求める
S412
原画像データGを複数のブロックに分割する
S413
各ブロックの平均値Cijを求める
S414
公開情報埋込部となるブロックを判別する
S415
秘密情報埋込部と無情報埋込部とを決定する
S416
秘密情報埋込部と無情報埋込部とからデータD2を検出する
S417
データD2を誤り訂正符号化し、パリティデータD3を生成する
S418
パリティデータD3を秘密情報埋込部に埋め込む
S419
END

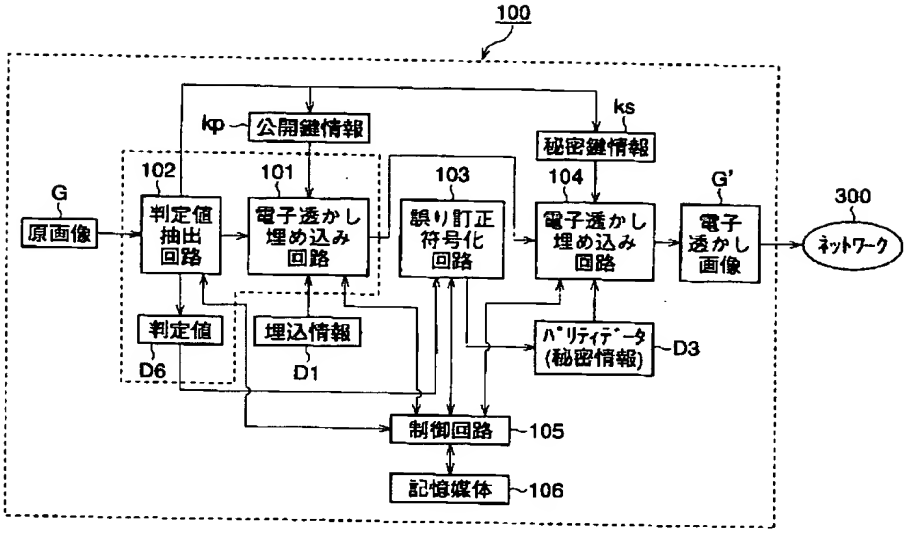
【図６】


D1
埋込情報
107
誤り訂正符号回路
D1'
符号化埋込情報
原画像G
電子透かし埋め込み回路
101
公開鍵情報kp
(a)
D1
埋込情報
ks'
秘密鍵
108
暗号化回路
D1"
暗号化埋込情報
原画像G
電子透かし埋め込み回路
101
公開鍵情報kp
(b)

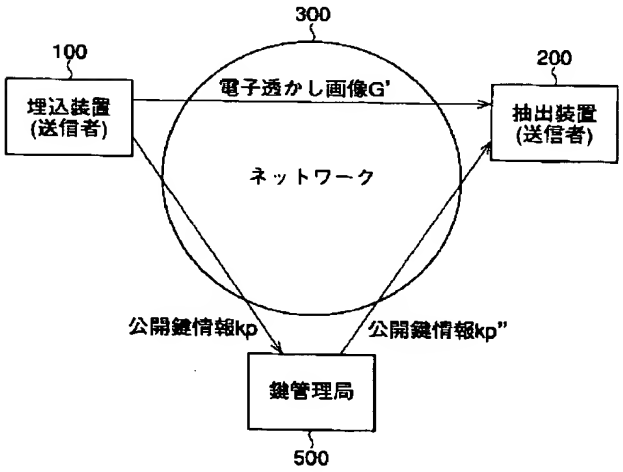
【図８】


300
100
埋込装置(送信者)
電子透かし画像G'
公開鍵情報kp
200
抽出装置(送信者)
ネットワーク

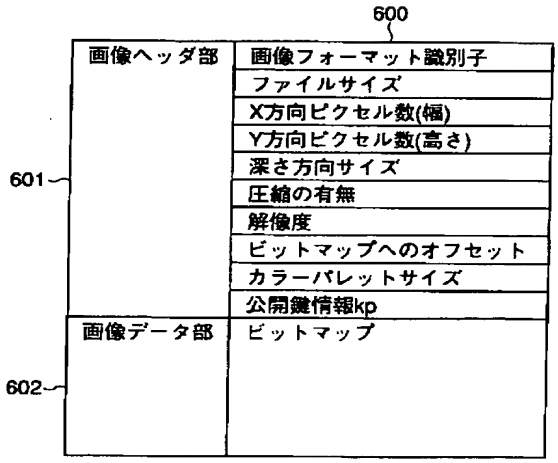
【図７】


100
kp
公開鍵情報
ks
秘密鍵情報
102
101
103
104
G
G'
300
原画像
判定値抽出回路
電子透かし埋め込み回路
誤り訂正符号化回路
電子透かし埋め込み回路
電子透かし画像
ネットワーク
判定値
D6
埋込情報
D1
ﾊﾟﾘﾃｨﾃﾞｰﾀ(秘密情報)
D3
制御回路
105
記憶媒体
106

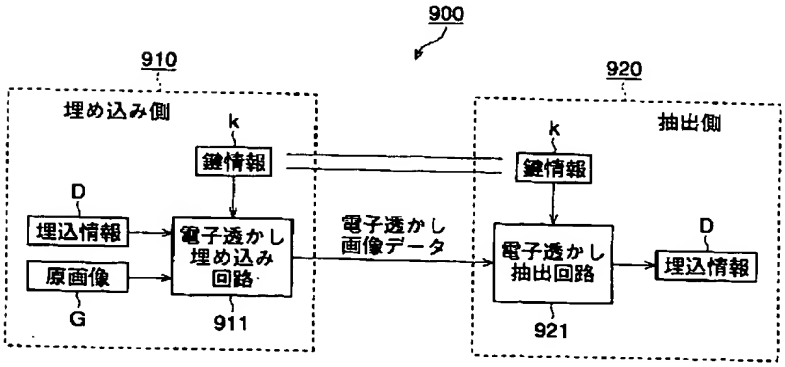
【図９】


300
100
200
埋込装置(送信者)
電子透かし画像G'
抽出装置(送信者)
ネットワーク
公開鍵情報kp
公開鍵情報kp"
鍵管理局
500

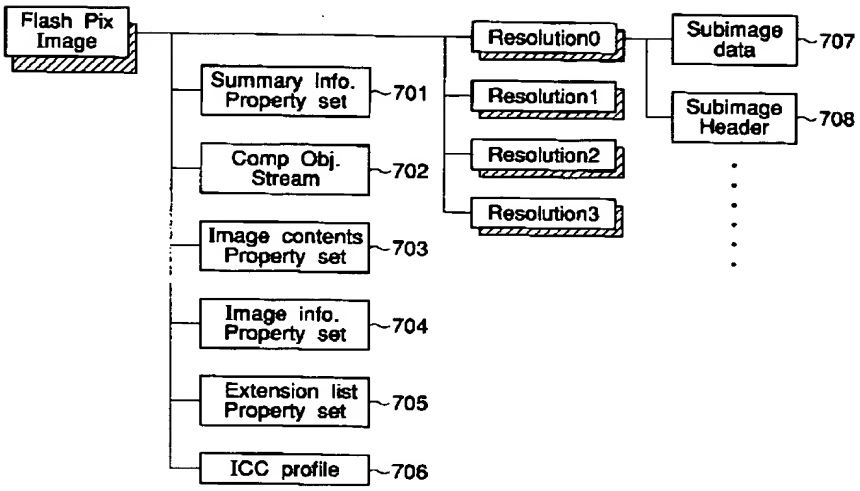
【図１０】


600
画像ヘッダ部
画像フォーマット識別子
ファイルサイズ
X方向ピクセル数(幅)
Y方向ピクセル数(高さ)
深さ方向サイズ
圧縮の有無
解像度
ビットマップへのオフセット
カラーパレットサイズ
公開鍵情報kp
601
画像データ部
ビットマップ
602

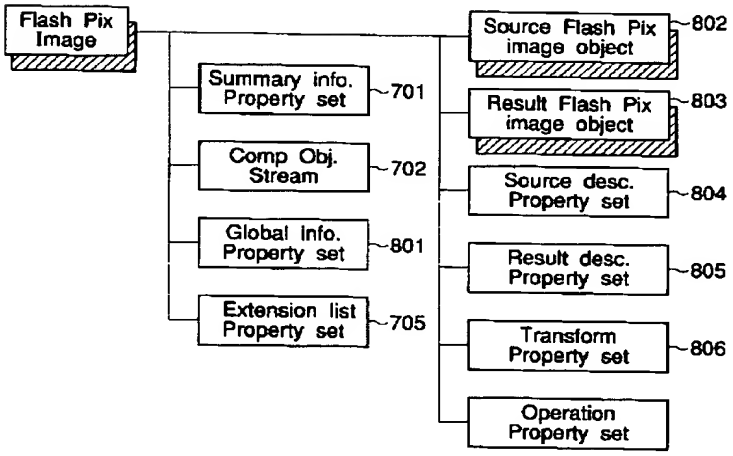
【図１４】


900
910
920
埋め込み側
抽出側
k
鍵情報
k
鍵情報
D
埋込情報
原画像
G
電子透かし埋め込み回路
911
電子透かし画像データ
電子透かし抽出回路
921
D
埋込情報

【図１１】


Flash Pix Image
Summary Info. Property set
701
Comp Obj. Stream
702
Image contents Property set
703
Image info. Property set
704
Extension list Property set
705
ICC profile
706
Resolution0
Resolution1
Resolution2
Resolution3
Subimage data
707
Subimage Header
708

【図１２】


Flash Pix Image
Summary info. Property set
701
Comp Obj. Stream
702
Global Info. Property set
801
Extension list Property set
705
Source Flash Pix image object
802
Result Flash Pix image object
803
Source desc. Property set
804
Result desc. Property set
805
Transform Property set
806
Operation Property set

【図１３】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4 | VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGﾃｰﾌﾞﾙのｲﾝﾃﾞｯｸｽ	0x03000002	VT_UI4